CLAIMS

1. A method for maintaining secure network connections, the method comprising:

detecting a change of address associated with a first network element;

updating at least one first security configuration at the first network element;

transmitting at least one secure message from the first network element to a second network element, wherein the at least one secure message comprises information associated with the change of address; and

updating at least one second security configuration at the second network element based at least in part on the at least one secure message.

2. The method according to claim 1, wherein a lookup of security associations is not dependent on any destination address.

3. The method according to claim 1, wherein the first network element is a mobile client and the second network element is a security gateway.

4. The method according to claim 1, wherein the first network element and the second network element are part of a virtual private network (VPN).

5. The method according to claim 1, wherein communications between the first network element and the second network element are based on a security architecture for the internet protocol (IPsec).

6. The method according to claim 5, wherein at least part of the communications between the first network element and the second network element are based on an internet security association and key management protocol (ISAKMP).

7. The method according to claim 6, wherein the second network element identifies at least one security association based on at least one cookie field in the at least one secure message.

8. At least one signal embodied in at least one carrier wave for transmitting a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 1.

9. At least one processor readable carrier for storing a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 1.

10. A method for maintaining secure network connections, the method comprising:

duplicating, between a second network element and a third network element, information associated with a secure network connection between a first network element and the second network element, wherein a lookup of security associations associated with the secure network connection is not dependent on any destination address; and

replacing the second network element with the third network element in the secure network connection with the first network element.

11. The method according to claim 10 further comprising sending at least one secure message from the third network element to the first network element.

12. A method for maintaining secure network connections, the method comprising:

configuring a plurality of security gateways such that a lookup of security associations is not dependent on any destination address; and

sharing at least one security association among the plurality of security gateways.

13. A system for maintaining secure network connections, the system comprising:

means for detecting a change of address associated with a first network element;

means for updating at least one first security configuration at the first network element;

means for transmitting at least one secure message from the first network element to a second network element, wherein the at least one secure message comprises information associated with the change of address; and

means for updating at least one second security configuration at the second network element based on the at least one secure message.

14. The system according to claim 13, wherein a lookup of

security associations is not dependent on any destination address.

15. The system according to claim 13, wherein the first network element is a mobile client and the second network element is a security gateway.

16. The system according to claim 13, wherein the first network element and the second network element are part of a virtual private network (VPN).

17. The system according to claim 13, wherein communications between the first network element and the second network element are based on a security architecture for the internet protocol (IPsec).

18. The system according to claim 17, wherein at least part of the communications between the first network element and the second network element are based on an internet security association and key management protocol (ISAKMP).

19. The system according to claim 18, wherein the second network element identifies at least one security association

based on at least one cookie field in the at least one secure message.